RESTRICTIONS ON GOVERNMENT ACCESS TO HEALTH INFORMATION

[*45 CFR Part 160, Subpart C; 164.512(f)*]

Background

Under the HIPAA Privacy Rule, government-operated health plans and health care providers must meet substantially the same requirements as private ones for protecting the privacy of individual identifiable health information. For instance, government-run health plans, such as Medicare and Medicaid plans, must take virtually the same steps to protect the claims and health information that they receive from beneficiaries as private insurance plans or health maintenance organizations (HMO). In addition, all Federal agencies must also meet the requirements of the Privacy Act of 1974, which restricts what information about individual citizens – including any personal health information – can be shared with other agencies and with the public.

The only new authority for government involves enforcement of the protections in the Privacy Rule itself. To ensure that covered entities protect patients' privacy as required, the Rule requires that health plans, hospitals, and other covered entities cooperate with efforts by the Department of Health and Human Services (HHS) Office for Civil Rights (OCR) to investigate complaints or otherwise ensure compliance.

RESTRICTIONS ON GOVERNMENT ACCESS TO HEALTH INFORMATION

Frequently Asked Questions

Q: Does the HIPAA Privacy Rule require my doctor to send my medical records to the government?

A: No. The Rule does not require a physician or any other covered entity to send medical information to the government for a government data base or similar operation. This Rule does not require or allow any new government access to medical information, with one exception: the Rule does give the Department of Health and Human Services Office for Civil Rights (OCR) the authority to investigate complaints that Privacy Rule protections or rights have been violated, and otherwise to ensure that covered entities comply with the Rule.

For enforcement purposes, OCR may need to look at how a covered entity handled medical records and other personal health information, as is typical in many enforcement settings. This investigative authority is needed so that the Rule can be enforced, and to ensure the independent review of consumers' concerns over privacy violations. Even so, the Privacy Rule limits disclosures to OCR to information that is "pertinent to ascertaining compliance." OCR will maintain stringent controls to safeguard any individually identifiable health information that it receives. If covered entities could avoid or ignore enforcement requests, consumers would not have a way to ensure an independent review of their concerns about privacy violations under the Rule.

Q: Why would a HIPAA Privacy Rule require covered entities to turn over anybody's personal health information as part of a government enforcement process?

A: An important ingredient in ensuring compliance with the Privacy Rule is the Department of Health and Human Services' (HHS) responsibility to investigate complaints that the Rule has been violated and to follow up on other information regarding noncompliance. At times, this responsibility entails seeing personal health information, such as when an individual indicates to the Department that they believe a covered entity has not properly handled their medical records.

What information would be needed depends on the circumstances and the alleged violations. The Privacy Rule limits HHS Office for Civil Rights' (OCR) access to information that is "pertinent to ascertaining compliance." In some cases, no personal health information may be needed. For instance, OCR would need to review only a business contract to determine whether a health plan included appropriate language to

protect privacy when it hired an outside company to help process claims.

Examples of investigations that may require OCR to have access to protected health information include:

- Allegations that a covered entity refused to note a request for correction in a patient's medical record, or did not provide complete access to a patient's medical records to that patient.

- Allegations that a covered entity used health information for marketing purposes without first obtaining the individuals' authorization when required by the Rule. OCR may need to review information in the marketing department that contains personal health information, to determine whether a violation has occurred.

Q: Will this HIPAA Privacy Rule make it easier for police and law enforcement agencies to get my medical information?

A: No. The Rule does not expand current law enforcement access to individually identifiable health information. In fact, it limits access to a greater degree than currently exists, since the Rule establishes new procedures and safeguards that restrict the circumstances under which a covered entity may give such information to law enforcement officers.

For example, the Rule limits the type of information that covered entities may disclose to law enforcement, absent a warrant or other prior process, when law enforcement is seeking to identify or locate a suspect. It specifically prohibits disclosure of DNA information for this purpose, absent some other legal requirements such as a warrant. Similarly, under most circumstances, the Privacy Rule requires covered entities to obtain permission from persons who have been the victim of domestic violence or abuse before disclosing information about them to law enforcement. In most States, such permission is not required today.

Where State law imposes additional restrictions on disclosure of health information to law enforcement, those State laws continue to apply. This Rule sets a national floor of legal protections; it is not a set of "best practices."

Even in those circumstances when disclosure to law enforcement is permitted by the Rule, the Privacy Rule does not require covered entities to disclose any information. Some other Federal or State law may require a disclosure, and the Privacy Rule does not interfere with the operation of these other laws. However, unless the disclosure is required by some other law, covered entities should use their professional judgment to

decide whether to disclose information, reflecting their own policies and ethical principles. In other words, doctors, hospitals, and health plans could continue to follow their own policies to protect privacy in such instances.

Q: Does the HIPAA Privacy Rule create a government database with all individuals' personal health information?

A: No. The Privacy Rule does not create such a government database or require a physician or any other covered entity to send medical information to the Federal government for a government database or similar operation.

Q: How does the HIPAA Privacy Rule affect my rights under the Federal Privacy Act?

A: The Privacy Act of 1974 protects personal information about individuals held by the Federal government. Covered entities that are Federal agencies or Federal contractors that maintain records that are covered by the Privacy Act not only must obey the Privacy Rule's requirements but also must comply with the Privacy Act.